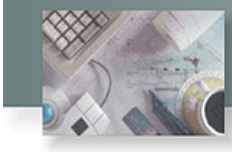

Compliance Component

DEFINITION	
Name	Virtual Private Networks (VPNs)
Description	Virtual Private Networks (VPNs) are combinations of software and hardware that allow site-to-site and site-to-client secure communications over public or untrusted mediums to establish a secure private connection with the agency network.
Rationale	Virtual Private Networks (VPNs) provide an alternative to building a private network for site-to-site communication or dial-in access. Because they operate across a shared infrastructure rather than a private network, agencies can cost-effectively extend the agency network to locations that may not have been justified before.
Benefits	• Provide opportunities for increased productivity of mobile employees, telecommuters, business partners and remote sites by allowing access to agency resources • Provide confidentiality and integrity of the data in transport through the public connection • May reduce cost to provide network access to remote users or sites • Allow traffic to be aggregated into a single connection rather than having multiple independent circuits terminating at the agency access point

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Infrastructure
Specify the Discipline Name	Remote Access
Specify the Technology Area Name	Virtual Private Network (VPN)
Specify the Product Component Name	None

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	None

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	Virtual Private Networks (VPN) must meet all requirements specified by the Security Domain VPN Compliance Component. Hardware must support split tunneling. Hardware must support 3DES or AES standards. Hardware must support access control lists. Hardware must support pre-shared keys or certificate authentication. Hardware must support remote management. Hardware must support network address translation (NAT) and port address translation (PAT). Hardware must support static IP addresses and site to site VPN routing.

	Hardware must support static routing. Hardware must support two factor authentication Hardware configurations must be configurable thru a command line interface. Hardware should support authentication of users. Hardware should support out-of-band management. Hardware should support content filtering. Hardware should support Open Shortest Path First (OSPF) or other standards based dynamic routing protocols. Hardware configurations should be configurable thru a web based or client based software. VPN remote client software must meet the Security Domain CC for VPNs.
Document Source Reference #	NIST Special Publication 800-46, Security for Telecommuting and Broadband Communications; NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems; NIST Special Publication 800-77, Guide to IPSec VPNs.

Compliance Sources

Name	NIST	*Website*	www.csrc.nist.gov
Contact Information			
Name		*Website*	
Contact Information			

KEYWORDS

List Keywords	Access control list, Virtual Private Network (VPN), routing, remote mgmt, Broadband, Cable, DSL, Wireless, Broadband over Power Line (BPL), Power Line Communications (PLC), Satellite, Modem, Internet, Dial-up, Telecommute, Mobile, Roadwarrior, Remote, IPSec, Tunnel, Site-to-Site, Site-to-Client.

COMPONENT CLASSIFICATION

Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*
Sunset Date	

COMPONENT SUB-CLASSIFICATION

Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☐ *Variance*		
☐ *Conditional Use*		

Rationale for Component Classification			
Document the Rationale for Component Classification			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	11-3-2005	*Date Approved / Rejected*	3/14/06
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	2/2/06
Reason for Update			